Cloudturing

클라우드 보안 백서

꿈많은청년들 CTO
cto@cloudturing.com

2025년 12월 15일

Abstract

본 문서는 Cloudturing 플랫폼의 클라우드 보안 아키텍처와 데이터 보호 정책을 설명합니다. Google Cloud Platform(GCP)을 기반으로 구축된 본 서비스는 다중 계층 보안 전략, 암호화된 통신, 체계적인 접근 제어를 통해 기업과 기관의 데이터를 안전하게 보호합니다. 이 백서는 기술적 세부 사항과 함께 보안 정책의 핵심 원칙을 다룹니다.

Contents

1 개요

1.1 서비스 소개

Cloudturing는 비개발자도 쉽게 AI 챗봇을 생성하고 배포할 수 있는 노코드/로우코드 AI 챗봇 빌더 플랫폼(SaaS)입니다. Google의 Gemini AI를 활용하여 인텐트(의도)를 자동으로 생성하고 학습시키며, 웹사이트에 간단한 스크립트 삽입만으로 즉시 배포할 수 있습니다.

1.2 보안 원칙

Cloudturing는 다음과 같은 핵심 보안 원칙을 준수합니다:

1. **최소 권한 원칙 (Principle of Least Privilege)**
   모든 서비스 계정과 사용자는 업무 수행에 필요한 최소한의 권한만 부여받습니다.
2. **심층 방어 (Defense in Depth)**
   네트워크, 애플리케이션, 데이터 계층에 걸쳐 다중 보안 레이어를 적용합니다.
3. **기본 암호화 (Encryption by Default)**
   전송 중인 데이터와 저장된 데이터 모두 암호화를 기본으로 적용합니다.
4. **제로 트러스트 (Zero Trust)**
   네트워크 경계에 의존하지 않고, 모든 요청에 대해 신원 확인과 권한 검증을 수행합니다.

1.3 클라우드 인프라

본 서비스는 Google Cloud Platform(GCP)을 기반으로 운영되며, 주요 인프라 구성 요소는 다음과 같습니다:

구성 요소	설명
클라우드 플랫폼	Google Cloud Platform (GCP)
컨테이너 오케스트레이션	Google Kubernetes Engine (GKE) Autopilot
주 리전	asia-northeast3 (서울)
로드 밸런서	Google Cloud Load Balancer (GCLB)
관계형 데이터베이스	Cloud SQL for PostgreSQL
분석 데이터베이스	BigQuery
캐시/세션 저장소	Valkey (Redis 호환)

Table 1: 인프라 구성 요소

2 접근 제어 및 인증

2.1 통합 계정 관리 (Google Workspace)

사내의 모든 계정 관리는 **Google Workspace(GWS)**를 통해 중앙 집중식으로 관리됩니다. 이를 통해 다음과 같은 보안 이점을 확보합니다:

- 2단계 인증(2FA) 강제 적용
- 조직 단위의 계정 수명주기 관리
- 보안 키 및 FIDO2 인증 지원
- 실시간 로그인 모니터링 및 이상 탐지
- 퇴사자 계정 즉시 비활성화

SSO(Single Sign-On) 연동
Google Workspace 계정을 통해 GCP Console, Cloud SQL, GKE 등 모든 클라우드 리소스에 통합 로그인합니다. 별도의 비밀번호 관리가 필요 없어 보안 취약점을 최소화합니다.

2.2 역할 기반 접근 제어 (RBAC)

서비스 계정과 사용자 권한은 업무 역할에 따라 명확히 분리됩니다:

역할	권한 범위
`Manager`	데이터베이스 읽기/쓰기, 스토리지 관리, AI 플랫폼 접근, Kubernetes 클러스터 조회
`Reader`	데이터베이스 읽기 전용, 스토리지 객체 조회, BigQuery 데이터 조회
`CloudBuilder`	CI/CD 빌드 실행, 아티팩트 저장소 푸시, 로그 기록

Table 2: 역할별 권한 분리

2.3 서비스 계정 관리

애플리케이션 레벨에서는 용도별로 분리된 서비스 계정을 사용합니다:

- `manager`: 관리/쓰기 작업용 서비스 계정
- `reader`: 읽기 전용 작업용 서비스 계정
- `cloud-builder`: CI/CD 파이프라인 전용 서비스 계정

각 서비스 계정은 필요한 최소 권한만 부여받으며, GKE 내에서는 **Workload Identity**를 통해 Pod와 서비스 계정 간 안전한 매핑을 수행합니다.

2.4 데이터베이스 접근 제어

Cloud SQL(PostgreSQL) 데이터베이스 접근은 **Cloud IAM 그룹 기반 인증**을 사용합니다:

- 데이터베이스 비밀번호 대신 IAM 토큰 인증 사용
- Google Workspace 그룹 멤버십에 따른 접근 권한 자동 부여
- 개인 계정이 아닌 그룹 단위 권한 관리로 일관성 확보

3 네트워크 보안

3.1 네트워크 아키텍처

프라이빗 네트워크 기본 원칙
모든 내부 서비스 통신은 프라이빗 네트워크 내에서 이루어지며, 외부 인터넷에 직접 노출되지 않습니다.

3.1.1 VPC 네트워크 구성

- **프라이빗 GKE 클러스터**: 모든 노드가 외부 IP 없이 프라이빗 IP만 사용
- **VPC Peering**: Google 관리 서비스(Cloud SQL 등)와 프라이빗 연결
- **Cloud NAT**: 아웃바운드 트래픽에 대한 중앙 집중식 IP 관리 및 로깅

3.1.2 네트워크 세그먼트

네트워크 영역	용도	격리 수준
Master Network	GKE 컨트롤 플레인	완전 격리
Pod Network	애플리케이션 Pod 간 통신	클러스터 내부 전용
Services Network	Kubernetes 서비스	클러스터 내부 전용
Managed Services	Cloud SQL, Cloud Storage 등	VPC Peering

Table 3: 네트워크 세그먼트 구성

3.2 방화벽 정책

GKE 클러스터 보안을 위해 세부적인 방화벽 규칙을 적용합니다:

1. **Master Node 연결 허용**: 컨트롤 플레인과 노드 간 HTTPS/gRPC 통신만 허용
2. **Pod 간 통신 허용**: 동일 클러스터 내 Pod 간 트래픽 허용
3. **로드밸런서 헬스체크 허용**: Google 로드밸런서 IP 범위에서의 헬스체크 트래픽 허용
4. **내부 네트워크 허용**: 10.0.0.0/8 대역 내 통신 허용
5. **Kubelet 읽기 전용 포트 차단**: 보안 취약점이 있는 포트 10255 차단

기본으로 생성되는 불필요한 방화벽 규칙(SSH, RDP 등)은 클러스터 생성 시 자동으로 삭제됩니다.

3.3 Cloud Armor (DDoS 방어)

Google Cloud Armor를 통해 애플리케이션 계층 보호를 제공합니다:

- **ASN 기반 차단**: 알려진 악성 트래픽 소스 차단
- **속도 제한**: 비정상적인 요청 빈도 제한
- **지리적 차단**: 필요시 특정 국가/지역 차단 가능

3.4 외부 접점 보안

외부에서 서비스에 접근하는 유일한 경로는 **Google Cloud Load Balancer(GCLB)**입니다:

- IPv4 및 IPv6 이중 스택 지원
- 전역 Anycast IP를 통한 DDoS 완화
- Cloud Armor 정책 적용점
- SSL/TLS 종단점

4 데이터 보호 및 암호화

4.1 전송 중 데이터 암호화 (Data in Transit)

모든 네트워크 통신은 암호화됩니다:

통신 구간	암호화 방식
클라이언트 ↔ 로드밸런서	TLS 1.2/1.3 (HTTPS)
로드밸런서 ↔ GKE	Google 내부 암호화
애플리케이션 ↔ Cloud SQL	SSL 전용 모드 적용
애플리케이션 ↔ BigQuery	Google 내부 암호화

Table 4: 구간별 암호화 방식

4.1.1 SSL 인증서 관리

Google Certificate Manager를 통해 SSL 인증서를 자동으로 관리합니다:

- 와일드카드 SSL 인증서 자동 발급 및 갱신
- DNS 기반 도메인 소유권 검증
- 인증서 만료 전 자동 교체
- 운영/개발 환경 별도 인증서 관리

4.1.2 데이터베이스 SSL 정책

Cloud SQL 인스턴스는 `ssl-mode: ENCRYPTED_ONLY` 설정으로 생성되어, 모든 연결에 SSL 암호화를 강제합니다. 비암호화 연결 시도는 거부됩니다.

4.2 저장된 데이터 암호화 (Data at Rest)

Google Cloud Platform에서 저장되는 모든 데이터는 자동으로 암호화됩니다:

- **Cloud SQL**: AES-256 기본 암호화, 고객 관리 암호화 키(CMEK) 옵션 지원
- **Cloud Storage**: AES-256 서버 측 암호화
- **BigQuery**: AES-256 기본 암호화
- **GKE 영구 디스크**: AES-256 기본 암호화

암호화 키 관리
Google Cloud의 기본 암호화 키 관리 서비스(KMS)를 사용하여 암호화 키를 안전하게 저장하고 주기적으로 교체합니다.

4.3 백업 및 복구

4.3.1 데이터베이스 백업

Cloud SQL 인스턴스에 대해 자동 백업 정책을 적용합니다:

- 일일 자동 백업 (매일 UTC 19:00, KST 04:00)
- 백업 보관 기간: 7일
- 백업 저장 위치: asia (아시아 리전)
- 자동 스토리지 확장 활성화

4.3.2 포인트-인-타임 복구

Cloud SQL의 바이너리 로깅을 통해 특정 시점으로의 복구가 가능합니다.

5 감사 및 모니터링

5.1 로그 수집 체계

서비스 운영에 필요한 모든 로그는 BigQuery에 중앙 집중식으로 저장됩니다:

로그 유형	기록 내용
`Login`	사용자 로그인 시간, 접속 IP, 인증 방식
`Usage`	챗봇 사용 기록, 채널, 인텐트 매칭
`AI Usage`	AI API 호출 기록, 토큰 사용량, 모델 정보
`Web Chatbot Usage`	웹챗 위젯 접속 기록, 페이지 URL
`Chatbot Usage`	챗봇 설정 변경 이력
`Audit Log`	시스템 감사 로그, 크레딧 사용 내역

Table 5: 로그 유형별 기록 내용

5.2 데이터 보관 정책

- **운영 환경**: 2년(730일) 보관 후 자동 삭제
- **개발 환경**: 30일 보관 후 자동 삭제
- **월별 파티셔닝**: 효율적인 데이터 관리 및 조회 최적화
- **클러스터링**: 주요 필드 기준 데이터 정렬로 쿼리 성능 향상

5.3 Cloud NAT 로깅

아웃바운드 네트워크 트래픽에 대한 상세 로그를 기록합니다:

- 모든 NAT 트래픽에 대한 로깅 활성화
- 소스/대상 IP, 포트, 프로토콜 기록
- 비정상 트래픽 패턴 탐지에 활용

5.4 감사 추적

사용자 및 시스템의 주요 활동에 대한 감사 추적을 제공합니다:

- 챗봇 생성/수정/삭제 이력
- 인텐트 학습 및 변경 이력
- AI 크레딧 사용 내역
- 권한 변경 이력

6 운영 보안

6.1 환경 분리

운영(Production)과 개발(Development) 환경을 완전히 분리합니다:

구분	운영 환경	개발 환경
도메인	cloudturing.com	********.com
SSL 인증서	별도 인증서	별도 인증서
로그 보관	2년	30일

Table 6: 운영/개발 환경 분리

6.2 유지보수 정책

- **GKE 클러스터 및 OS 보안**: GKE 노드는 Google에서 직접 관리하고 최적화한 Container-Optimized OS를 사용합니다. OS 레벨의 취약점이나 보안 이슈가 발견될 경우, Google의 관리형 서비스를 통해 자동으로 최신 보안 패치가 적용된 이미지로 업데이트됩니다. 이를 통해 인프라 레벨의 보안 위협을 선제적으로 차단합니다.
- **보안 알림 및 대응 체계**: Google Cloud의 주요 보안 업데이트 및 공지사항(RSS)을 Slack과 연동하여 실시간으로 모니터링합니다. 긴급 보안 패치나 중요 업데이트 알림 수신 시, 운영팀이 즉각적으로 내용을 파악하고 프로덕션 환경에 빠르게 적용하는 대응 프로세스를 구축하고 있습니다.
- **Cloud SQL**: 운영 유지보수 채널을 사용하며, 트래픽이 적은 일요일 새벽 시간대에 유지보수 창을 설정하여 가용성을 보장합니다.

6.3 CI/CD 보안

Cloud Build를 통한 안전한 배포 파이프라인:

- 전용 서비스 계정으로 빌드 실행
- 빌드 로그 별도 저장소에 보관
- Artifact Registry를 통한 컨테이너 이미지 관리
- GKE 배포 권한과 빌드 권한 분리

7 규정 준수

7.1 GCP 보안 인증

Cloudturing는 다음과 같은 보안 인증을 보유한 Google Cloud Platform 위에서 운영됩니다:

- ISO/IEC 27001 (정보보안 관리체계)
- ISO/IEC 27017 (클라우드 보안)
- ISO/IEC 27018 (클라우드 개인정보 보호)
- SOC 1/2/3 (서비스 조직 통제 보고서)
- CSA STAR (클라우드 보안 연대)

7.2 데이터 주권

7.2.1 저장 데이터

- 모든 **고객 데이터**(사용자 정보, 챗봇 설정, 대화 기록, 학습 문서 등)는 **대한민국 서울 리전 (asia-northeast3)**에 저장
- Cloud SQL, BigQuery, Cloud Storage 등 모든 저장소가 국내 리전에 위치
- 국내 데이터 보호 규정 준수

7.2.2 AI 추론 데이터

AI 챗봇 응답 생성을 위해 Google Vertex AI API를 사용하며, 다음과 같은 정책이 적용됩니다:

- AI 추론 요청 시 데이터는 Google의 글로벌 인프라에서 처리
- Google은 유료 Vertex AI 서비스의 고객 데이터를 **AI 모델 훈련에 사용하지 않음**
- 추론 완료 후 입력 데이터는 **영구 저장되지 않음**
- 악용 모니터링 목적의 임시 로그만 제한된 기간 보관 (정책 위반 탐지용)
- Google Cloud Data Processing Addendum 적용

AI 데이터 보호 정책
Google Vertex AI는 유료 서비스에 대해 고객의 프롬프트와 응답을 모델 개선에 사용하지 않습니다. 처리된 데이터는 추론 완료 후 삭제되며, 고객 데이터의 원본은 항상 국내 서울 리전에만 저장됩니다.

8 부록

8.1 용어 정의

용어	설명
GKE	Google Kubernetes Engine, 컨테이너 오케스트레이션 서비스
VPC	Virtual Private Cloud, 가상 사설 네트워크
IAM	Identity and Access Management, 신원 및 접근 관리
NAT	Network Address Translation, 네트워크 주소 변환
TLS	Transport Layer Security, 전송 계층 보안
RBAC	Role-Based Access Control, 역할 기반 접근 제어
SSO	Single Sign-On, 통합 인증
2FA	Two-Factor Authentication, 2단계 인증
DDoS	Distributed Denial of Service, 분산 서비스 거부 공격
SaaS	Software as a Service, 서비스형 소프트웨어

8.2 문서 이력

버전	날짜	변경 내용
1.0	2025년 12월 15일	최초 작성
1.1	2025년 12월 16일	GKE 보안 정책 및 업데이트 프로세스 추가

Table 8: 문서 이력

Cloudturing
본 문서에 대한 문의: cto@cloudturing.com